International Research Journal of Management and Commerce
ISSN: (2348-9766)
Impact Factor- 5.564, Volume 4, Issue 8, August 2017
Website- www.aarf.asia, **Email** : editor@aarf.asia , editoraarf@gmail.com

CYBER FRAUD ANDE-BANKING IN INDIA

Shipra Mishra
Research Scholar,Faculty of Commerce
Banaras Hindu University

ABSTRACT

'Necessity is the mother of invention', today this statement is truly applicable to all over the world, because each and every country wants to become the self sufficient and for this Information Technology plays an important role. Today all the works perform with the single click. E-banking is one of the best examples of the Information Technology to send or receive the money from one place to another without going to the bank branch. It makes the banking activities more easy and convenient to perform all over the world. Use of internet in banking activities increases the risk of cyber crime because the excess use of anything increases the misuse of the same, thus the cyber crime is the misuse of technology to theft the other money by illegal means. Thus the present paper discuss about the various aspects of e-banking and cyber crime risk in India. In this paper we highlights the present status of e-banking and cyber crime in India and for this we collect last five year data from various secondary sources such as websites, journals, magazine, RBI data, National Crime Record Bureau (NCRB), Indian Computer Emergency Response Team (CERT- In) report, IT Act, IPC Act, report and many more. Paper concluded that in India e-banking and cyber crime have a positive relationship and increases in the same direction due to the low literacy rate and less awareness about the use of user ID and password. We also highlight guidelines or some securities measures outline by RBI.

Keywords: Information Technology (IT), E-banking, Cyber Crime, National Crime Record Bureau (NCRB), Indian Computer Emergency Response Team (CERT-In), Reserve Bank of India (RBI).

Introduction

Electronic banking is one of revolutionary way of performing banking transactions in all spare of banking arena. Performing banking transaction electronically is a normal course of action. After Core banking solution (CBS); each and every bank is carried out the banking transaction effectively and efficiently. All the banking personnel in both public and private sector bank are well equipped with adequate skill straining to carry out banking transactions electronically. At present due to the various initiatives of Union Government, E-banking is growing in all parts of the country equally and economically and in the same direction, the RBI has taken and framed various guidelines and regulation to stabilize all e-banking activities systematically. The major hurdles that restrict the e-banking transaction are lack of education exposure on e-banking transactions by the customers. Till date the government has taken various steps to eradicate this problem but due to some implementation problem, the government did not get success in these aspects. Besides, customers, the employees and government norms restrict the working of e-banking system efficiently.

After implementation of electronic transaction the growth of banking in different aspects such as income, profit, number of transactions value of transaction and transaction per hour. The real beneficiary is both customers as well as the banking system. E-banking reduces the cost and time of both sides (customer and banks) leads to higher satisfaction and the main focus of this paper is to identify the ways performing e-banking, performance achieved and point out the various hurdles in executive banking transaction. Further, this paper provides some solution to rectify the various problems faced by the bankers as well as customers.

E-banking

In India all banks offers various services to their customers, i.e., accepting and deposit customer money, granting loans and providing various other banking services to customers. E-banking services allows a bank’s customers and other stakeholder to interact and transact with the bank seamlessly through a variety of channels such as the internet, wireless device, ATMs, online banking, Tele-banking and Mobile banking. E-banking refers to the use of technology which allows customers to perform banking transaction electronically without visiting a branch or institutions.

E-banking includes Electronic Fund Transfer (EFT), Electronic Clearing Services (ECS), Immediate Payment System (IMPS) and various other services. Online banking helps consumers to overcome the limitation of the branch banking, through these customers can bank anywhere, anytime as these services are available 24*7 without any physical limitation. They also bypass the paper based aspects of traditional banking.**United National Conference on Trade and Development (UNCTAD)** defines E-banking as **"**internet banking refers to the development over the internet of retail and wholesale banking services. It involves individual and corporate clients and includes bank transfers, payments and settlements, corporate and household landings, card business and some other banking activities." E-banking introduced in India after 1990s, and credit of launching E-banking is goes to the ICICI bank which introduced various E-banking services in the year 1996. And after that all other public and private banks started the e-banking services.

E-banking Fraud

E-banking is now covered more than 50 percent population of the country, but the rest 50 percent population are not ready to adopt e-banking transaction due to low literacy rate and increases in cyber fraud in e-banking. Cyber crime in Indian banking sector are defined under cyber-deceptions. Cyber-deception mainly covered the immoral activities which include theft, Debit and credit card fraud, and intellectual property violations.In a simple term bank fraud defines, the use of various illegal means to obtain or theft other money, assets or other financial property which is held by the various banks or any financial institutions and its come under the criminal offence.

E-banking fraud is also called cyber crime in banking sectors. E-banking fraud use technology to theft or remove money from ones bank account, it also include the wrongly transfer of money from one account to another and many more activities. Banks provide user ID and password to perform E-banking transactions, but due to the less knowledge or awareness about the use of password customers can easily falls into the trap of cyber criminals.

Types of E-banking fraud- There are many e-banking frauds used to taken place while performing this type of transaction and they are listed below-

1- Phishing,

a- Phishing over the phone,

b- Phishing by SMS,

2- Identity theft,

3- Viruses and Trojans,

4- Spyware and Adware,

5- Card Skimming,

6- EFTPOS skimming.

1- Phishing – "Phishing" is a form of Internet fraud that aims to steal valuable information such as card numbers, user IDs and passwords. A fake web site is created to look similar to that of a legitimate organization, typically a financial institution such as a bank or insurance company. An email or SMS is sent requesting that the recipient access the fake web site and enter their personal details, including security access codes. The page looks genuine but users entering information are inadvertently sending their information to the fraudster.

a-Phishing over the phone- Fraudsters don't only strike online. Phishing, where traditionally emails seek to represent a known or trusted entity and trick people into disclosing their account or personal details, is now increasingly happening over the phone. Be particularly vigilant if you’re asked to disclose any Internet Banking sign-in details or Secure Code sent to your mobile.

b- Phishing by SMS- Your mobile can be a target for fraudsters too. If you receive any SMS message that you have not requested or are expecting, and you're suspicious

2- Identity theft- It can take many forms, from fraudulent credit card use, to your entire identity being used to open accounts, obtain loans, and conduct other illegal activities. Be suspicious if anyone asks you for your personal information. Scammers use convincing stories to explain why you need to give them money or personal details.

3- Viruses and Trojans- Viruses and Trojans are harmful programs that are loaded onto your computer without your knowledge. The goal of these programs may be to obtain or damage information, hinder the performance of your computer, or flood you with advertising. Viruses spread by infecting computers and then replicating. Trojans appear as genuine applications and then embed themselves into a computer to monitor activity and collect information. Using a firewall and maintaining current virus protection software can help minimizes your chances of getting viruses and inadvertently downloading Trojans.

4- Spyware and Adware- When clicking on pop-up advertisements – ones that “pop up” in a separate browser window – it’s possible you are also downloading “spyware” or “adware”. These programs often come bundled with free programs, applications or services you may download from the Internet. Spyware or Adware software covertly gathers your user information and monitors your Internet activity, usually for advertising purposes.

5- Card skimming- Card skimming is the illegal copying and capture of magnetic stripe and PIN data on credit and debit cards. Skimming can occur at any bank ATM or via a compromised EFTPOS machine. Captured card and PIN details are encoded onto a counterfeit card and used to make fraudulent account withdrawals and transactions.

6- EFTPOS skimming-Electronic Funds Transfer at Point of Sale (EFTPOS). A foreign device is implanted into an EFTPOS machine that is capable of copying and capturing card and PIN details processed through the machine. A compromised EFTPOS terminal can only be detected by a physical inspection. **Job and employment scams-** Job and employment scams target people looking for a new job or a change of job. They often promise a lot of income (sometimes they even guarantee it) for not a lot of work. If you have received a work from home offer that you think could be a scam, or if you have responded to a job advertisement that you now realize is a scam.

These all types of e-banking fraud is registered under the three main boards of India i.e., Information Technology Act (IT Act) 2000, The Indian Penal Code (IPC) Act 1860 and State Level Legislations (SLL). The above e-banking fraud is punishable under the relevant provisions of the **Indian Penal Code, 1860** (as amended by the Information Technology Act, 2000). In India maximum cases are registered under the IT Act 2000, because all aspects of cyber crime is governed and controlled by this act. Under it misuse of information technology like hacking, introduction of viruses, phishing, card skimming and many more other cases are registered and also decide the crime level and presentment. Thus the IT Act is the main law dealing with cyber crimes in India. Cases registered under the following sections-

- Tampering computer source documents (Section 65 IT Act)
- Loss /damage to computer resource/utility (Section 66 (1) IT Act)
- Hacking (Section 66 (2) IT Act)
- Obscene publication/transmission in electronic form (Section 67 IT Act)
- Failure of compliance/orders of Certifying Authority (Section 68 I T Act)
- Failure to assist in decrypting the information intercepted by Govt. Agency (Section 69 IT Act)
- Unauthorized access/attempt to access to protected computer system (Section 70 IT Act)
- Obtaining license or Digital Signature Certificate by misrepresentation / suppression of fact (Section 71 IT Act)
- Publishing false Digital Signature Certificate (Section 73 IT Act)
- Fraud Digital Signature Certificate (Section 74 IT Act)
- Breach of confidentiality/privacy (Section 72 IT Act)

Literature Review

Business Standard(July 2015)- With the increase in banking on mobile phones and the internet, financial frauds in the system have also seen an uptick, says a survey on financial frauds in the financial sector by Assocham and PwC. The report said that financial frauds led to approximately $20 billion (Rs 1.26 lakh crore) in direct losses annually. The report states that currently, 74 per cent of the population has mobile phones and this has led to a steady rise in banking on the go. According to Reserve Bank of India data, the volume of mobile banking transactions has risen from around Rs 1,819 crore in 2011–12 to approximately Rs 1,01,851 crore in 2014-15. Whether it's financial transactions, customer experience, marketing of new products or channel distribution, technology has become the biggest driver of change in the financial services sector. Most financial institutions are therefore insisting on cashless and paperless transactions.

Business Insider India (Jan 5, 2015) - consulting arm of Mahindra Group, suggests that the number of cyber crimes in the country is expected to double and cross the 3-lakh mark in 2015. As per the study, the cyber crimes are growing at a rate of 107% year on year while registering over 12,000 cases every month. According to the report, the number of cases of cyber crimes was 13,301 cases in the year 2011, which was followed by 22,060 such cases in 2012 and 71,780 cases in 2013. By May 2014 alone, the cyber cells in India had registered a whopping increase in cyber crime cases and registered 62,189 cases. The increasing use of mobile, smart phones, tablets for online banking and financial transactions has also increased the vulnerabilities to a great extent. The maximum offenders came from the 18-30 age groups, stated the report. The economic growth of any nation and its security whether internal or external and competiveness depends on how well is its Misuse of the ATM-cum-debit card had been a common problem for all. Often debit card users report fraudulent transactions have been made through their ATM cards even when the cards were in their possession

Objectives of the study

The main objective of the present study is as follows-

1. To Study the E-banking services in India.
2. To study about the various types of E-banking frauds or Cyber fraud in India.
3. To analyze the present status of e-banking fraud in India.

Research Methodology

The present study is mainly focused on secondary data and the data is collected by the various secondary sources such as journals, newspaper, magazine, and from various websites. The collected data is the summarized and analyzed by the chart and graphs. For this we have collected 5 years data from 2011 to 2015.

Present status of E-banking fraud in India

According to the IAMAI (Internet and Mobile Association of India) and IMRB International report on "Internet in India 2015", report India is the second highest user of internet, after US, with the 402 million users of Internet in December 2015 and its users has increased by 49% as compared to last year. China has the largest internet user base, with over 600 million users. In India with the increase in internet users, e-banking transactions also increase at the high rate, but at the same time it also increases the cyber crime in country. According to the National Crime Records Bureau (NCRB) report on cyber crime, defines the number of cyber crime record or registered in India has gone up more than 4 times in last 5 years.The main reason of this is the absence of proper security system and unawareness about the use of technology and safe use of password. In between 2011-2015 India registered more than 32000 cases relate to the cyber crime, under the various acts such as IT Act 2000, IPC act 1860 and in State Legal Legislation (SLL). In India most of the cases are registered in IT Act 2000 it also recorded the person arrested. Table-1 shows the cyber crime registered and person arrested in India in Between 2011-2015.

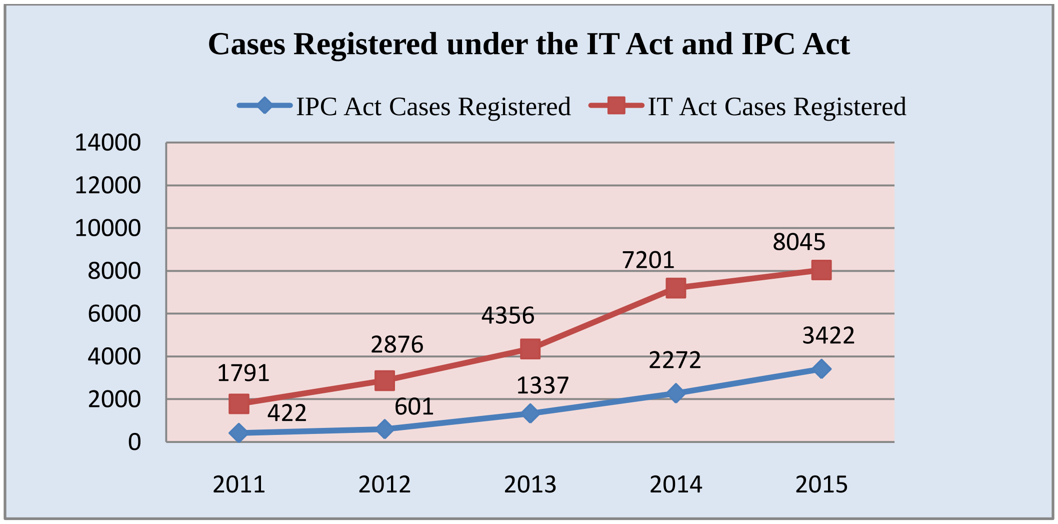
Table-1 Cases registered in cyber crime in India

Cases registered	2011-12	2015-16	Growth Percentage (%)
Under IT Act 2000	1791	8045	449.19%
Under IPC Act 1860	422	3422	810.90%

Sources- National Crime Record Bureau (NCRB) Cyber Crime Statistics

In the above table it is observed that there is a huge growth percentage recorded in both act. IT Act 2000 records more than 400% increase in the cases registered in cyber crime in India and IPC Act record more than 800% growth in between 2011 to 2015. Cases registered under IT Act for the last five years are- **1791 (2011-12), 2876 (2012-13), 4356 (2013-14), 7201 (2014-15), 8045 (2015-16).** Thus the total cases registered under IT Act in between 2011-2015 is **24,269**, on the other hand cases registered under the IPC Act for last five year i.e. **2011 to 2015 is 422 (2011-12), 601 (2012-13), 1337 (2013-14), 2272 (2014-15), 3422 (2015-16)** and total cases registered under IPC Act is 8054 from 2011-2015. These five year cyber crime trends are shown by the graph-1.

Graph-1 Cases registered under IT Act and IPC Act



Sources: National Crime Records Bureau (NCRB) Cyber Crime Statistics in India 2015

From the above data it is observed that cyber crime in India increases day to day; it means that it has a positive relationship with the e-banking transactions. India ranked third pace after Japan and US, as countries most affected by cyber crime or online banking frauds. So it increases the demand of proper and good security system to cover the cyber crime in India. NCRB also issues data related to the person arrested under the both act which is shown by the following table.

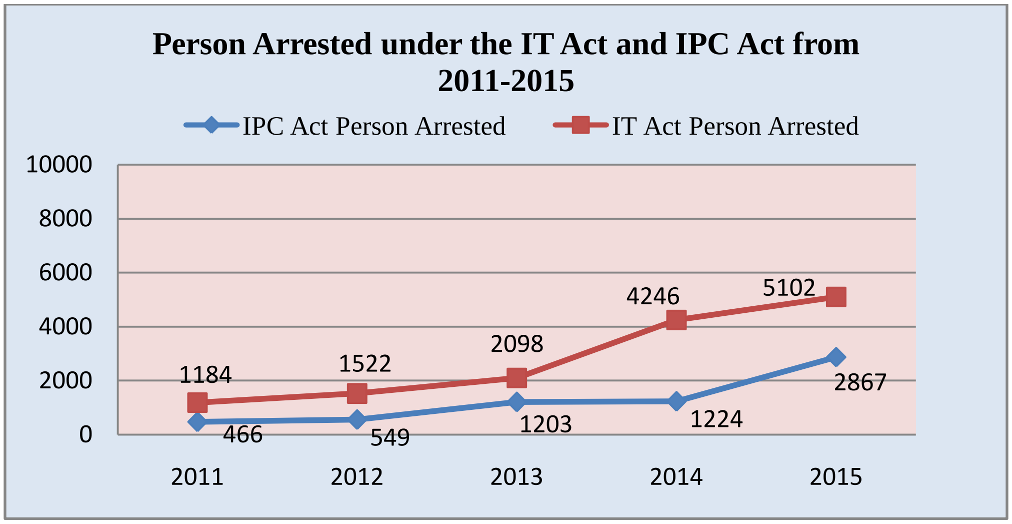
Table-2 Person Arrested under cyber crime in India

Person Arrested	2011-12	2015-16	Growth Percentage (%)
Under IT Act 2000	1184	5102	430.91%
Under IPC Act 1860	446	2867	642.83%

Sources- National Crime Record Bureau (NCRB) Cyber Crime Statistics

Table-2 shows the person arrested under the IT Act and IPC Act. Last 5 years data of person arrested under the IT Act 2000 are **1184 (2011-12), 1522 (2012-13), 2098 (2013-14), 4246 (2014-15), 5102 (2015-16).** Thus the total person arrested from 2011 to 2015 is 14152 and it record more than 400% growth in between 2011-2015. At the same time person arrested under IPC Act 1860, is **446 (2011-12), 549 (2012-13), 1203 (2013-14), 1224 (2014-15), 2867 (2015-16)**thus the total number of person arrested under the IPC Act is 6289 and it record more than 600% growth. The trend of growth in between 2011-2015 is shown by the graph-2.

Graph-2 Person Arrested under IT Act and IPC Actfrom 2011-2015



Sources: National Crime Records Bureau (NCRB) Cyber Crime Statistics in India 2015

Thus from the above two tables, it is concluded that cyber crime in India increases at the very high rate and it become the very big problem for the country, because India is going towards the Digitalization. As a developing country India should have been a good policy for the regulating and controlling for the cyber crime.

In India, RBI the apex body of Indian baking system and Indian Computer Emergency Response Team (CERT-In) also recorded the cyber securities related crime. RBI disclosed the various ATM, Debit Card, Credit Card, Internet banking or all virtual banking related crime, according to the RBI in the last four year more than 46000 cases are registered such as 8765 cases in the year 2012-13, 9500 in the year 2013-14, 13083 (2014-15) and more than 15000 cases in 2015-16. CERT-In data on Cyber fraud for last three year is 44679 (2014), 49455 (2015) and 50362 (2016) respectively. The cases registered under the CERT-In are related to the various Phishing, scanning or Probing, virus or Malicious code, website intrusion, malware and many others.

NCRB also records cyber crime data on the basis of state wise because, it helps to know the most affected state with cyber crime. In India UP and Maharashtraare the top 2 states in cyber crimes these two states records the highest number of cyber crimes in India. Some most affected state with cyber crime in e-banking is discussed in the table-3.

Table-3 State wise cyber crime registered and person arrested in India (2011-2015)

State	Cases Registered	Person Arrested
Maharashtra	5935	3088
Uttar Pradesh	4990	3868
Rajasthan	2243	920
Madhya Pradesh	1162	1093
Kerala	1680	958
Karnataka	3597	888
Andhra Pradesh	2295	1577
West Bengal	1461	847

Sources: National Crime Records Bureau (NCRB) Cyber Crime Statistics in India 2015

From the table-3 it is observed that, in India UP, Maharashtra, Karnataka and Andhra Pradesh are the top four states which record the highest number of cases registered under the IT Act and

IPC Actand it also record the highest number of person arrested.On the other hand Madhya Pradesh and West Bengal registered record the least number of cyber crime from 2011 to 2015.

RBI's circular for minimizing Cyber Crime in banks

RBI, the apex banking institution of India defines some measures to control the cyber crime in banking industries. RBI circular to banks urges them to take adequate measures that are robust and resilient which address and tackle risks posed by cyber criminals, and in the meantime also put in place an adaptive Incident Response Management and Recovery (IRMR) framework to deal with adverse disruptions if and when they occur.

Protecting customers- Banks are required to put in place strong controls to protect customer data across the life cycle regardless of whether data is at rest or in motion, within the bank's environment or within the vendor's environment. As banks are rapidly adopting digital products, they are also mandated to take stronger measures in areas such as authentication and risk-based transaction monitoring to prevent fraud. Banks have also been asked to establish strong programmes focused on customer awareness to reduce the incidence of attacks such as phishing.

24*7 security operations centre with adaptive threat defense mechanisms- There is a need for effective cyber security monitoring and detection capabilities that focus on building resilient systems that traverse a large volume of system events and deduce intelligence. A resilient banking ecosystem is characterised by banks' ability to detect threats in advance, prevent cyber incidents, recover from an incident should one materialise and learn from threat intelligence to prevent similar incidents. Banks will have to refocus some of their security operations priorities and augment their current security operations centre (SOC) to make it more robust by focusing on cyberthreats on a real-time basis.

Establishment of strong governance and cyber awareness board- Banks will need to create programmes and interventions in order to sensitize the board and management about the evolving threat landscape and the current and future state of their cyber security posture. This will help in setting the right tone at the top. The circular clearly calls for greater participation of the board. No longer can they just be a ratifying body and instead they will need to be more involved and keep abreast about the latest cyber security developments and accordingly provide necessary guidance and insights.

Focus on extended ecosystem-There is also a clear recognition that information cuts across boundaries and it is no longer adequate to have strong controls with respect to security within the bank and a light touch approach to the vendor ecosystem. The circular calls for strong governance over the entire vendor life cycle with respect to cyber security. Banks would need to embed into their relationship with all vendors the right to audit and the fact that they may be subjected to review by the regulator itself.

Building cyber resilience- As attack vectors are increasingly becoming sophisticated, the cost of launching an attack is going down, the scale and velocity of attacks are increasing, and there is greater recognition of the possibility of incidents. Accordingly, banks not only need to strengthen cyber defence but also build strong resilience. The RBI circular calls for the establishment of a Cyber Crisis Management Plan to address the full life cycle of detection, response, containment and recovery.

Proactive reporting and collaboration- In its circular, RBI has recognised that collaborating and contributing financial institutions can benefit mutually and further help others to make informed decisions, thus enabling them to respond to attacks proactively and quickly. In many ways, the circular will move the industry to a new evolved state with respect to cross-leveraging learning's from one another.

Conclusion and suggestions

Thus from the above discussion it is clear that E-banking is a new feather in the cap of the Indian banking sectors. It reduces the time and effort to perform banking activities but on the other hand it is very risky to perform because of the absence of a good security system. Security is the most significant issue in E-banking. It may arise in the form of unauthorized access of key information of bank account. Many people are still not comfortable with online portals, especially from the security point of view. In addition to this, banks also face the internal problems like employee frauds. Trust of customer in a web venture is an important concern. Many customers hesitate to deal with an online bank as they are not sure of the quality of products and services they will receive. The paper also concluded that e-banking and cyber crime are increases simultaneously and it is required to make a good security system to protect the e-banking transactions.

References

1. www.ncrb.nic.in
2. www.rbi.org.in
3. www.timesofindia.Indiatimes.com
4. www.ijsrp.ogr
5. AgrawalSachin (2016), “Cyber Crime in Banking Sector”, UdgamVigyati – The Origin of Knowledge Cyber Crime in Banking Sector, volume 3, IISN 2455-2488.
6. Aggarwal, Gifty (2015), General Awareness on Cyber Crime. International Journal of Advanced Research in Computer Science and Software Engineering, August Vol 5, Issue 8.
7. Joshi, S. Mayur (2016), Full Guide on Cyber Crimes in India. Article published in “Cyber Fraud Resources”. Journal of Frauds, India Forensic Consultancy Services.
8. 8. Mehta, Saroj&Singh,Vikram (2013), A Study of Awareness About Cyberlaws in the Indian Society. International Journal of Computing and Business Research, January, Vol.4, Issue. 1.
9. Avais, M. Abdullah et.al.,(2014), Awareness regarding cyber victimization among students of University of Sindh, Jamsharo. International Journal of Asian Social Science, Vol. 4(5): 632-641
10. Crime in India: 2011-Compendium (2012), National Crime Records Bureau, Ministry of Home Affairs, Government of India, New Delhi, India.
11. Cyber Law & Information Technology (2011) by Talwant Singh, Additional District & Sessions Judge, New Delhi, India.
12. Introduction to Indian Cyber Law (2008) by RohasNagpal, Asian School of Cyber Laws, Pune, India.
13. Cyber Crime (2003) by R.K. Suri and T.N. Chhabra, Pentagon Press, New Delhi, India.